Overview and Features of Generic Security Protocols for Cloud Computing Environment

Rashid Husain

***Abstract* - In this research paper we are describing the several generic protocols use in Cloud computing environment. Now-a-days Cloud Computing has become very important in large and small enterprise so security has also become very important for Cloud Computing. Several technique use to protect the cloud. Techniques are implemented by protocols. This paper is based on overview of protocols that use in Cloud computing environment. The protocols of cloud computing can also use in different security system such as Cryptonet System, Mailing System and Authentication System.**

***Index Terms* –** Authorization, Cloud Computing, Cryptographic, CryptoNET, Encryption, Protocol, Security

I. Introduction

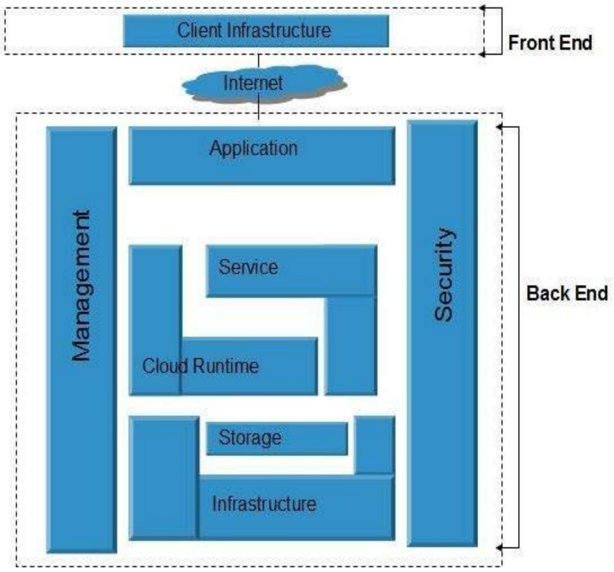
Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the software as a service (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centers. Moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management [1]. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) are both well-known examples. While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. As a result, users are at the mercy of their cloud service providers for the availability and integrity of their data [1], [2]. From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons. . Firstly, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted due to the users' loss control of data under Cloud Computing. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Considering various kind of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging. Secondly, Cloud Computing is not just a third party data warehouse [3].

II. Cloud Computer Architecture

Cloud Computing architecture comprises a set of cloud components, which are loosely coupled. We can broadly divide the cloud architecture into two parts [20]:

- Front End
- Back End

Each of the ends is connected through a network, usually Internet. The following diagram shows the graphical view of cloud computing architecture:



Front End

The **front end** refers to the client part of cloud computing system. It consists of interfaces and applications that are required to access the cloud computing platforms, Example - Web Browser.

Back End

The **back End** refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge data storage, virtual machines, security mechanism, services, deployment models, servers, etc.

III. Importance of Cloud Computing on Enterprises

Now-a-days cloud computing became very important in the information technology domain. Despite its popularity, there are many enterprises are implementing and utilizing cloud

Rashid Husain, Senior Lecturer, Department of Mathematics and Computer Sciences, Umaru Musa Yar'aduva University, Katsina, Nigeria

computing for business and operating purpose due to the existing vagueness regarding its cost and security effect associated. The main attractiveness of cloud computing for organizations is its cost effectiveness, while the major concern relates to the risks for security. Security is major problem associated with cloud computing in enterprises. Moreover, several major implications that enterprise should keep in mind while using cloud computing and provides security protocol on how to avoid the cost and security risks identified [21]. The term "cloud-computing" is used for describing both a platform and type of applications. Users and enterprises information is saved in the cloud on servers. The term is also used for applications which are made accessible through Internet. Cloud applications are stored in large data centers on powerful servers which host web applications and web services [22]. Many information technology players, such as Google, Amazon, Microsoft, etc., are using to developing and offering cloud services [21].

IV. Benefits of Cloud Computing on Enterprises

There are many benefits of cloud computing on enterprises but some are very close such as [23]:

Cost Benefits

- Reduce spending on technology infrastructure
- Reduce capital cost
- Associated saving
- Convenience saving

Technical Benefits

- Minimize upkeep
- Innovation in technology
- Devise diversity
- Easy implementation
- Customization
- Increased storage

Business-level Benefits

- Customization
- Flexibility
- Agility
- Innovation
- Choice and quality of service
- Monitoring
- Staying ahead of the curve

V. Features of Generic Security Protocols

Generic security protocols are enabling components of our security system that provide network security services to various components of the Cloud computing environment. These protocols are: initial local user authentication protocol, remote user authentication protocol, Single-Sign-On protocol, consuming protocol, cloud trust protocol, secure sessions protocol, file transfer protocol [7],[8].

Design of the protocols is based on the concepts of generic security objects and modular approach. Each protocol is complete in terms of its functionality, each is easy to integrate with other components, and each transparently handles security credentials and attributes. In addition, they provide the same set of secure network services to all components of the cryptonet system [9], [15].

VI. Design of Security Protocols on Cloud Computing

Design of security protocols is based on modular approach and each module is implemented using the concept of generic security objects. This section describing the overview of generic protocols used in cloud computing and some other security system such as cryptonet system [15].

A. File Transfer Protocol

Cloud can store many different type of files that can be use in enterprise. A file can contain any type of digital information-text document, image, art work, movie, sound, software etc. hence anything that can be stored on a computer can be moved with FTP service [4]. FTP used as a standard protocol to transfer files from one computer over Internet. The users can send the file on the cloud using FTP. The user's information includes user name, the password, and the home directory. FTP use as a distribution system that can retrieve both local and cloud file. FTP used to put locking system on cloud information as well as local system [5].

B. Local User Authentication Protocol

Local user authentication protocol is use in cloud computing and other types of security system.

Local user authentication protocol is designed as a login module. It supports username/password-based authentication, and certificates based authentication. Upon starting the system, the workstation automatically checks installation environment and its configuration and then selects the appropriate protocol. If it is configured for username/password-based authentication, our system acquires PIN and/or PIN plus fingerprint from a user in order to activate. It fetches username and password from the Security Applet and presents them to the login module of the native operating system. Login module consults user accounts database for authentication [15], [19].

C. Consuming Protocol

This protocol is designed for specially consumer and provider. This protocol describe in terms of security, reliability, privacy. Cloud computing provides services to businesses and consumer in sense of cost-effective, scalable, flexibility and proven delivery platforms. Software-as-a-service (Saas) can reduce the overall cost of hardware and software development, maintenance activity. Platform-as-a-service (Paas) can minimize the cost and complexity of buying, housing, and handling the software and hardware components of the platform. So consuming protocol is also important feature whenever design cloud computing architecture. Many small and big enterprises are now using cloud computing as a consumer [8].

D. Remote User Authentication Protocol

Cloud computing is a new pattern of computing system which enables the users to transfer their work to the cloud. The adoption of cloud computing is emerging rapidly, the security and privacy issues are still significant challenges. Cloud computing is open resource means a user accesses the information to the cloud server through open networks. So many types of security problem can be started if a secure system is not established. User's personal information may be exposed to an attacker. Therefore, user anonymity is also an important concern in cloud computing. Remote user authentication protocol use in security technique to establish a secure transfer in cloud system [11].

E. Secure Cloud Transmission Protocol

Cloud computing technologies have become very important because of its several benefits. Now small and big business organization using cloud computing services to cut the cost and complexity of their business. There are need to provide secure transmission. There are certain security issues in cloud computing environment to overcome security issues, secure transmission is needed. Secure transmission cloud protocol apply in transmission control protocol (TCP) and user datagram protocol (UDP). It is considered a state of the art protocol, which promptly addresses various infrastructure requirements for transmitting data in high speed network. Now secure cloud transmission protocol are based on UDP-based data transport protocol (UDT) [9], [10].

F. Cloud Trust Protocol

The Cloud Trust Protocol (CTP) is the technique by which cloud user ask for and receive digital information as applied to cloud service provider. This protocol use to establish a trust on cloud's owner. This protocol can be use to establish a security technique on cloud computing environment. This protocol can use in nature of digital trust. Digital trust provides the security of digital information. Transparency of information is at the root of digital trust, and thus the source of value capture and payoff. CTP is use to establish digital trust between a cloud computing customer and provider and create transparency about the provider's configuration vulnerabilities, authorization, accountability and operating status conditions [6], [7].

G. Secure Single-Sign-On Protocol

Cloud computing and cloud protocol is the dominant and highly paced technology of present scenario with the highly robust service infrastructure that can provide cloud based integrated services like service on demand for resource computation, storage or cumulative storage of recourse or data and exceedingly vigorous network communication in the cloud technology [16]. For getting the proficient cloud based services over Internet services it can provide a swift and decidedly proficient system with least resource administration activities and minimum interface of service providers. Most of current application requires the client memorize and utilize different set of credentials to access. It is difficult for a corporation to manage potentially multiple authentication solutions and database individually used by each operation [17]. So we need a proper protocol that can make the sign on in easy way resulted single sign on protocol. In a single-on protocol, the clients can perform a single sign on to an identity provider trusted by application he/she wants to access an application. Single sign on protocol eliminate the need for clients to repeated prove their identities to different applications and hold different authentication for different applications [17].

H. Secure Sessions Protocol

After single-sign-on protocol successfully established, secure session protocol start to provide a session in cloud computing as well as other security system. Secure session protocols establish with key exchange certificate. The idea of the key exchange certificate is to securely exchange session-key and session-id between a client and cloud Server. Session protocol use session key to manage secure sessions' attributes at the application server. A session key is an encryption and decryption key that is randomly generated to ensure the security of a communications session between a user and another computer or between client and server. Session key also called symmetric keys, because the same key is used for both encryption and decryption. A session key derive from a hash value, using the cryptderive key function, this method is called a session key derivation scheme. Throughout session, the key is transmitted along with each message and is encrypted with the recepient's public key because much of their security relies upon the briefness of their use, session keys are changed frequently. A different session key may be used for each message [15], [18].

I. Authorization Protocol

Authorization protocol enables the technique in cloud computing environment to secure the authorization for consumer and service provider. Authorization policies in our security system are based on the XACML standard. We adopted Role-Based Access Control model, so an authorized person (for example Security Administrator (SAd)), creates a group and defines access level for each group member along with his/her role and permitted actions. SAd generates a Policy Token which includes Target object used to identify the role of each group member in a group. *Target* contains the name of a group member, the name of a resource, and actions permitted to perform by a group member with the specified resource authorization policy [15], [18].

J. Key Management Protocol

Some of secure applications in the cryptonet system and cloud computing operate in a collaborative environment and use key exchange protocol to exchange group-key between group members. For this purpose, we designed Generic Key Distribution (GKD) component compliant with the GSAKMP standard. GKD performs key-related functions like key creation, key distribution, and rekeying. GKD supports both Push and Pull-based operations to distribute shared-key. In addition, it works with Secure Application Server in order to perform key-distribution functions [15]. This module works with application servers as a component, so it uses PEP component of a host application server for enforcement of authorization policies for shared-keys. When a group member requests a group-key, he/she performs Single-Sign-On, and establishes secure session with Secure Application Server.

After that, group member fetches SAML ticket from a smart card and sends it to the PEP associated with the Secure Application Server. After successful authorization, GKD sends group-key to the authorized group member using secure communication channel. Cryptographic keys fall into two broad categories: (i) secret key (ii) Public/private key pair. There are some additional key uses in a cloud computing environment such as public/private authentication key pair, public/private signature key pair, public/private key establishment pair, symmetric encryption/decryption key, symmetric message authentication code key and symmetric key wrapping key [15], [19].

VII. Conclusion

We designed Security Protocols for authentication, secure communication and authorization between various components of Cloud computing system. Our protocols are based on the concept of generic security objects, well-established security standards and technologies. They transparently handle security credentials and handle protocol-specific attributes in cloud computing environment. In addition, the same attributes can be used by our designed protocols. Our generic security protocols are initial user authentication protocol, remote user authentication protocol, Single-Sign-On, secure sessions, file transfer protocol, cloud transmission protocol and key management protocol.

References

[1] Amazon.com, (2008). “Amazon Web Services (AWS)”, [Online], Aailable: http://aws. amazon.com.

[2] N. Gohring, (2008). “Amazon’s S3 down for several hours”, [Online], Aailable: http://www.pcworld.com/businesscenter/article/142549/amazons s3 down for several hours.html.

[3] A. Juels and J. Burton S. Kaliski, (2007). “PORs: Proofs of Retrievability for Large Files,” *Proc. of CCS ’07*, pp. 584–597.

[4] Sinha P.K and Sinha P. (2003), “Computer Fundamentals”, BPB Publications.

[5] Babu Ch. M. and Chandana O.L. (2014), “File transfer protocol in cloud computing,” [Online], Available: www.ijritcc.com

[6] Cloud security alliance, [Online], Available: www.cloud securityalliance.org/grp/cloudtrust-protocol/

[7] Cloud trust protocol (CTP), [Online], Available: searchcloudsecurity.techtaget.com

[8] Udagepola, etal., (2015). “a case study cloud computing consumer protocol in Australia”, journal of applied environmental and biological sciences.

[9] Secure cloud transmission protocol, [Online], Available: www. Tchrepublic.com

[10] Danilo Valeros Bernardo and Doan B Hoang, (2010). “ Securing data transfer in the cloud through introducing identification packet UDT-authentication option field: a characterization, [Online], Available: arxiv.org

[11] Z.Dong, (2014). “Security enhanced anonymous remote user authentication and key agreement for cloud computing, IEEE 17th international conference.

[12] H. Shacham and B. Waters, (2008). “Compact Proofs of Retrievability”, *Proc.of Asiacrypt*.

[13] K. D. Bowers, A. Juels, and A. Oprea, (2008). “Proofs of Retrievability: Theory and Implementation,” [Online], Aailable: http://eprint.iacr.org/.

[14] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, (2007). “Provable Data Possession at Untrusted Stores,” *Proc. Of CCS ’07*, pp. 598–609.

[15] Abbasi A. G., (2011), CryptoNET: Generic Security Framework for Cloud Computing Environments, Thesis in Communication Systems School of ICT.

[16] Cloud security alliance, “ security guidance for critical areas of focus in cloud computing V3.0, [Online], Available: www.cloudsecurity alliance.org

[17] Yaser fuad al-dubai and dr. khamitkar S.D., (2014). “Kerberos: secure single sign-on framework for cloud access control”, Global Journals Inc. USA

[18] Andre Patkos, “Session Key”, [Online], Available: www. Searchsecurity.techtarget.com

[19] Ramaswamy chandramouli, Michaela lorga and santosh chokhani, (2013). “ Cryptograhic key management issues & challenges in cloud services”, [Online], Available: nvlpubs.nist.gov

[20] Cloud Computing Architecture, [online], Available: www.tutorialspoint.com

[21] Mihail Dimitrov & Ibrahim Osman, “The impact of cloud computing on organizations in regards to cost and security”, [Online], Available: www.diva-portal.org

[22] Boss. G., Malladi P., Quan D., Legregani L. & Hall H., (2007). “Cloud Computing”, IBM Corporation.

[23] Benefits of Cloud Computing, (2012). [Online], Available: www.logicwork.net